



Mobile Device Security

Purpose:	To guide all barristers on good practice relating to mobile device security
Scope of application:	All barristers
Issued by:	The Information Technology Panel
Last reviewed:	April 2024
Status and effect:	Please see the notice at end of this document. This is not “guidance” for the purposes of the BSB Handbook I6.4.

1. Smartphones and tablets are a routine part of practice today. They can be used as a direct alternative to the desktop PC and may have much of the same functionality. Barristers may receive emails and attachments on a smartphone and may view these and reply using the same device. Files may be available to view and edit on smartphones. This can be convenient and time efficient. However, carrying information in this easily portable way comes with significant security risks.

2. The most obvious risk is that of loss (whether by chance or by theft). Whilst it used to be annoying to lose your contacts, losing a smartphone or tablet full of sensitive and privileged work emails and documents may have more serious consequences. Aside from the potential breach of the Rules of Professional Conduct (e.g. safeguarding client confidentiality in accordance with CD6 and rC15.5 of the Handbook) there may also be a personal data breach (See IT Panel Guidance, [Breaches – what to do when you lose papers, or when your data security is breached](#)). The information that some barristers routinely deal with can be special category data (e.g. medical reports, previous convictions), the loss of which may cause real distress to the people involved.

Minimising the risk

3. Prevent unauthorized access to your phone or tablet.

3.1.If your smartphone or tablet has an encryption function, this should be enabled.¹ Encryption greatly reduces the chance that someone can gain unauthorised access to the data even if they obtain the device. Prosecution case papers may only be stored on devices that have been encrypted (please see [here](#)) and the CJSM requirements to connect a mobile device to their network (please see [here](#)).

3.2.Use a unique code or password (preferably not a swipe gesture, as these are less secure, depending on the type of device you have) that is not easily guessed. Avoid 0000, 1111, 1234 etc. and do not re-use one that you use on other devices.

3.3.If your device also provides biometric security (fingerprint or face ID) this should be activated. Do not share your code with others or enable others' biometric use (e.g. adding a spouse's fingerprint to the unlocking profile).

3.4.Make sure you activate your device's screen lock function so that it locks within a short period of non-use.

3.5.If your device permits an automatic wipe after a certain number of failed access attempts, turn on this function.

3.6.Enable two-factor authentication for any work-related apps (e.g. apps on which you access work email or cloud storage apps). Your chambers or IT provider should be able to assist.

4. Reduce the amount of information that is permanently stored on the device. Most information in emails or cloud file storage can be downloaded from the cloud on an as-needed basis. Consider setting email storage to a period of time, such as 7 days or 1 month. Set cloud storage options to cloud-storage only, and download specific documents only when you need access to them. While you will need to retain emails and files for certain purposes (see the IT Panel Guidance, [Data Retention Policy](#)), do these really need to be on your portable smartphone or tablet that could easily be lost or stolen?

¹ Some devices are encrypted by default, e.g. iPhones and iPads - whenever the device is locked with a passcode, Touch ID or Face ID.

Commented [A1]: I'm unsure about this link – is it still the best one for our purposes, being from 2015 and apparently for civil panel counsel (not criminal prosecutors)?

Commented [A2R1]: This is still the correct document. I've checked and the CPS Panel requires a commitment to abide by these AG's guidelines (see <https://www.cps.gov.uk/advocate-panels> under the Tab panel member's commitments)

Commented [A3]: I think this is just me – grateful for any clarification – we have this link to v 1.2 of the “with MDM” policy, and in footnote 3 below we have a link to the “without MDM” policy. Having looked at both of these, I am a little confused about when each applies!

5. If your device has it, activate the find my phone function, so that you can find it if it is misplaced. iPhones and iPads have the software built-in (activate 'Find-my-iPhone'); Samsung has "Find my mobile". Similar software is available for Android and other handsets and tablets. These apps may also enable you to remote wipe the contents of the device if it is irretrievably lost. If you do lose your device, see the IT Panel Guidance - [Breaches – what to do when you lose papers, or when your data security is breached](#).

Connecting to the internet and charging your device

6. If you are not using a SIM card with a cellular data network provider, be careful how you connect to the internet on a mobile device. If using public wireless facilities your communications are potentially insecure. Not only could they intercept your e-mails, they could get your passwords too. If you must use a hotspot, make sure you do not set your tablet to 'auto-connect' to it. You may find your device logging on and transferring data insecurely when you do not know about it. If you can, use a VPN (virtual private network), or tether to a cellular network that is on another of your devices (a personal hotspot). Alternatively, use a dongle with its own SIM card that can connect directly to the cellular network (and then the internet) and create a personal hotspot. Make sure any personal hotspot is password-protected.

7. Avoid plugging your device into public USB-direct charging slots. A USB connection can transmit data without your knowledge or consent. Charge your device by plugging it into a normal power socket with the appropriate adaptor or a trusted device.

8. While working from your home network you need to make sure you have made it as secure as possible. A serious risk is that an online hacker might attempt to exploit poor Wi-Fi security measures and retrieve sensitive information or take advantage of your network to launch malicious attacks. You should consider:

- (i) Changing the default name of your Wi-Fi network, also known as the SSID (Service Set Identifier), makes it harder for malicious attackers to know what type of router you have. Try not to name it with information that could easily identify you or your location (e.g. "John's Wi-Fi" or "Bar Council Office").
- (ii) Set a strong and unique password to secure your wireless network. You should change the pre-set default username and password of the router which was provided by your supplier for the first installation. A long password is usually a strong password, so it should be around 20 characters long and include various numbers, letters and symbols or a phrase known only to you.

- (iii) Use a strong network administrator password to increase Wi-Fi security. You would have needed access to an online platform or website to set-up your wireless router, for which you would have been given the default access code by your supplier. Most Wi-Fi routers come with the default credentials such as “admin” and “your default password” which are easy for malicious hackers to break into, so these should be changed.
- (iv) Increase your Wi-Fi security by activating the network encryption. Ideally your network should be set to WPA3 or WPA2 (Wi-Fi Protected Access 2). For further information on how to encrypt your wireless network: see the information from Lifewire’s website [here](#).
- (v) Change your default IP address on the wireless router to create a further barrier for hackers. You should be able to change the IP address through the advanced settings on your [router administration platform/website](#).
- (vi) Check the security of all the IoT devices connected to your home network.

9. Be aware that some apps may require permissions which give them access to stored data on your device. You can monitor and change what permissions each app has in your security settings.

10. Ensure your device’s operating system is regularly updated. These updates usually contain security patches and bug fixes. Failing to install these can make your device susceptible to targeted attacks. This is easy if you ensure that the update facility is turned on, so that operating system updates are routinely managed.

11. As you would with any computer, do not download or open unexpected or suspicious emails/attachments/files/links. These can give hackers access to part or all of your device data. Be wary of installing unauthorised apps (i.e. not from the official app store). If your device allows, install an antivirus app to help protect from malicious software.

12. Do not store passwords/access codes in plain text on your device. Use a password manager. There are many different ones available for a variety of devices. This is a sensible investment. If you carry out any work for the CPS or government departments, you will have a secure e-mail address (CJSM) – it is a condition of being on any Government Panel. CJSM can now be used on a smartphone but only if you agree to set

up your phone securely. Strong passwords, screen-lock, full encryption, auto-erase if someone tries to break in, to name but a few.²

13. The storage of prosecution case papers on tablets (including those downloaded from the CCDCS) is likely to require the device to be properly encrypted.³ Encryption software may already be on your device - so make sure you enable it. I wouldn't want to be the one who is made an example of. You have been warned!

14. Apple's native Mail application on iPhones now offers the option of including attachments when replying to an email. You should check your settings for the native Mail application to ensure that the option "Include Attachments with Replies" is toggled to "Never" or "Ask".

Important Notice

This document has been prepared by the Bar Council to assist barristers on matters of information security. **It is not "guidance" for the purposes of the BSB Handbook I6.4, and neither the BSB nor a disciplinary tribunal nor the Legal Ombudsman is bound by any views or advice expressed in it. It does not comprise – and cannot be relied on as giving – legal advice.** It has been prepared in good faith, but neither the Bar Council nor any of the individuals responsible for or involved in its preparation accept any responsibility or liability for anything done in reliance on it. For fuller information as to the status and effect of this document, please see [here](#).

² The full terms and conditions can be found at

http://cjsm.justice.gov.uk/downloads/CJSM_Mobile_Security_Policy_non_MDM.pdf V1.3.

³ See ¶18 <https://www.gov.uk/guidance/attorney-generals-guidelines-on-information-security-and-government-work>